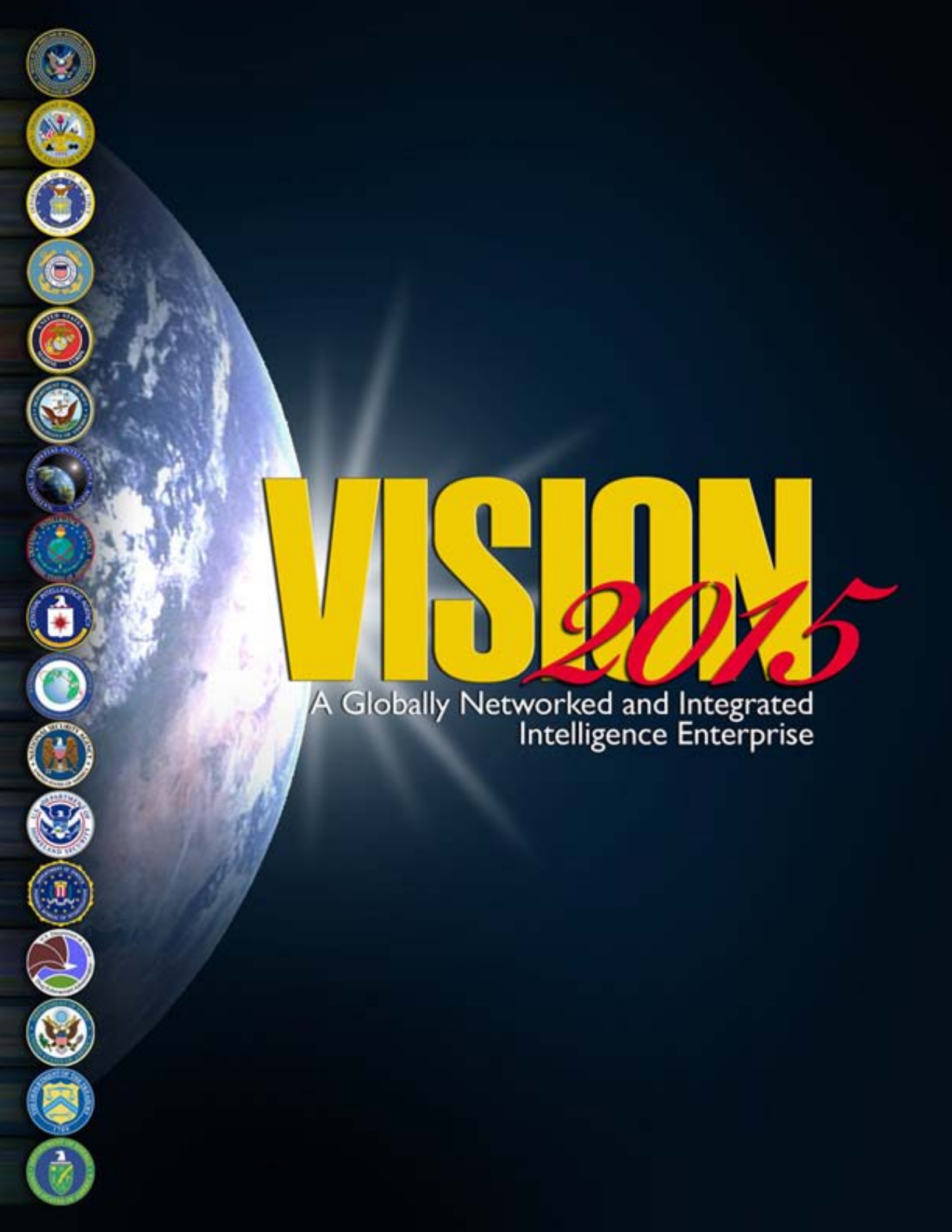

VISION 2015
A Globally Networked and Integrated
Intelligence Enterprise

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
01 JUL 2008		**00-00-2008 to 00-00-2008**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Vision 2105: A Globally Networked and Integrated Intelligence Enterprise	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Office of the Director of National Intelligence,Washington,DC**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**28**	

Mission

Create Decision Advantage

Vision

A Globally Networked and
Integrated Intelligence Enterprise

Strategy

Integrate foreign, military, and domestic intelligence capabilities through policy, personnel and technology actions to provide decision advantage to policy makers, warfighters, homeland security officials and law enforcement personnel

Values

Commitment • Courage • Collaboration

DIRECTOR OF NATIONAL INTELLIGENCE
WASHINGTON, DC 20511

Fellow Intelligence Professionals:

We are engaged in a dynamic global environment, in which the pace, scale, and complexity of change are unprecedented. It is a networked world where what happens in Peshawar affects Peoria — and vice versa. Risks are often unforeseen and threats are hidden and agile, making the job of intelligence professionals more critical and more challenging. Our national security depends on anticipating risks and out-maneuvering our adversaries, not just out-muscling them. Therefore, intelligence is more critical than ever. We must address these risks and threats by integrating all elements of national power — defense, homeland security, diplomacy, development, and intelligence. However, the Intelligence Community is still largely structured, staffed and operated around a design optimized for a different era. Adapting the Community to this new environment is our fundamental challenge. The purpose of this Vision document is to chart a new path forward for a globally networked and integrated Intelligence Enterprise for the 21st century based on the principles of integration, collaboration, and innovation.

The mission of the Intelligence Community is to create decision advantage for our customers — policymakers, military commanders, law enforcement and homeland security officials. This means we collect and analyze intelligence to improve our customers' ability to make a decision while denying our adversaries the same advantage. To transform the Community and create decision advantage, we will need to accomplish the following:

- Develop integrated capabilities to address emerging challenges in cyber space and support new missions such as energy security.
- Create a customer-driven intelligence model.
- Improve our ability to anticipate and prevent strategic surprise through better global awareness and strategic foresight.
- Integrate the Community through mission-focused operations that transcend agency and functional silos. This also requires us to network our collection assets to allow them to work, autonomously and cooperatively in near-real time, to penetrate the most difficult targets.
- Field a net-centric information enterprise that enables end-users to discover, access, and exploit intelligence information in a secure, tailored manner.
- Remove the barriers to cross-agency collaboration by integrating the strategic enablers of the Intelligence Enterprise — human capital, education and training, business systems, facilities, science and technology, and acquisition and procurement.

A vision without a map is just a wish. To make this Vision real, I challenge the Community's senior leaders, who participated in creating it, to develop a well-defined roadmap that details the steps we will take immediately, and throughout the next several years, to translate this Vision into reality. While our Vision extends to 2015, we must make real progress sooner rather than later. Our commitment to this Vision will be manifested in our budget priorities and implementation plans.

In 1996, the Chairman of the Joint Chiefs of Staff, General John M. Shalikashvili, published Joint Vision 2010, which detailed the conceptual template for our military forces. The document was brief, conceptual, and controversial, but it proved an effective guide for developing the superb military capabilities the United States now possesses. I invite all intelligence professionals to join in this fundamental transformation of our Community into an Intelligence Enterprise poised to continue to succeed for the foreseeable future.

J. M. McConnell


Innovation & Technology
Economic & Financial
Energy & Environment
GLOBALIZATION
Demographic & Health
Political & Military
Social & Cultural

1 THE SHIFTING STRATEGIC LANDSCAPE

Era of Uncertainty
Implications for the Intelligence Community

2 CREATING DECISION ADVANTAGE

3 MAKING IT REAL - IMPLEMENTING THE VISION

1 THE SHIFTING STRATEGIC LANDSCAPE

"When the rate of change outside your organization exceeds that within your organization, the end is near."

- Jack Welch, former CEO, General Electric

We live in a dynamic world in which the pace, scope, and complexity of change are increasing. The continued march of globalization, the growing number of independent actors, and advancing technology have increased global connectivity, interdependence and complexity, creating greater uncertainties, systemic risk and a less predictable future. These changes have led to reduced warning times and compressed decision cycles. Although this interconnected world offers many opportunities for technological innovation and economic growth, it also presents unique challenges and threats. In this environment, the key to achieving lasting strategic advantage is the ability to rapidly and accurately **anticipate and adapt to complex challenges**.

The integration of international politics and economics over the last century outpaced the integration of U.S. institutions. Our statecraft adapted over the decades with new policies and institutions. The future portends discontinuities with new threats from non-traditional actors, new modes of attack, and more lethal impact. Intelligence must be more integrated and agile to assist in preventing and responding to these challenges.

Era of Uncertainty

Many drivers and trends are shaping the future global environment in which the Intelligence Community must operate — demographic and social change, increased economic integration and competition, rapid technological innovation and diffusion, environmental pressures and growing energy demand, broad geopolitical changes and new forms of governance. Each driver and trend independently produces unique changes and challenges; those points where factors intersect often reinforce and amplify the effects of change and create a series of complex and often unpredictable threats and risks that **transcend geographic borders and organizational boundaries.**

Figure 1: Drivers and Trends

Global networks of information, finance, commerce, transportation, and people shape and empower these threats. This infrastructure increasingly is being targeted for exploitation, and potentially for disruption or destruction, by a growing array of state and non-state adversaries.

"We see globalization – growing interconnectedness reflected in the expanded flows of information, technology, capital goods, services and people throughout the world – as an overarching 'megatrend,' a force so ubiquitous that it will substantially shape all the other major trends in the world of 2020."

- National Intelligence Council, "Mapping the Global Future, 2020"

Persistent Threats

For the foreseeable future, we will act to prevent the next terrorist surprise, while addressing the root causes that fuel extremism. We will track the spread of technologies that enable individuals, groups, or rogue states to acquire weapons of mass destruction. We will compete with adversary foreign intelligence services to prevent exploitation of our security vulnerabilities. We will encounter deft attempts at denial and deception as we conduct our collection activities. Finally, we will monitor the economic, military, political and ideological dynamics of regional powers to identify and warn of impending challenges.

Emerging Missions

To these persistent threats we add a growing array of emerging missions that expands the list of national security (and hence, intelligence) concerns to include infectious diseases, science and technology surprises, financial contagions, economic competition, environmental issues, energy interdependence and security, cyber attacks, threats to global commerce, and transnational crime. Foremost among these challenges is the **blurring** of lines that once separated **foreign and domestic intelligence**, and the increased importance of homeland security. By necessity, we must be involved with numerous new partners in interactive relationships, but we must also **respect and maintain the privacy and civil liberties of all Americans**.

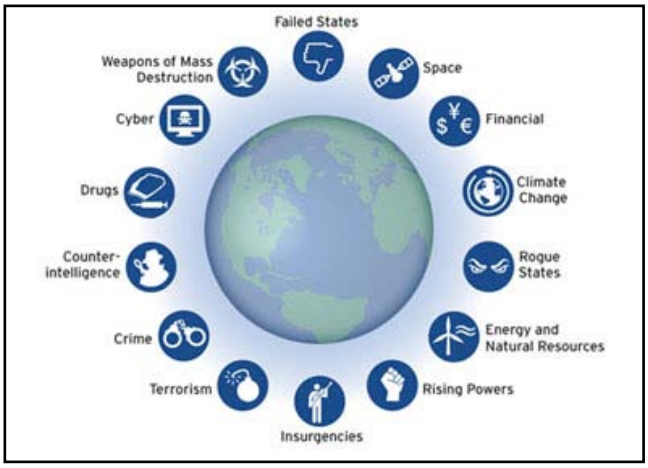


Figure 2: Persistent Threats and Emerging Missions

Old problems assume new dimensions: information operations with emphasis on a cyber domain, asymmetric political or military responses, and illicit trafficking. Lastly, we confront the challenge of acting in an environment that is more time-sensitive and open to the flow of information, in which intelligence sources and analysis compete in a public context established by a global media. By 2015 we will need integrated and collaborative capabilities that can anticipate and rapidly respond to a wide array of threats and risks.

Implications for the Intelligence Community

In this new environment, geographic borders and jurisdictional boundaries are blurring; traditional distinctions between intelligence and operations, strategic and tactical, and foreign and domestic are fading; the definitions of intelligence and information, analysts and collectors, customers and producers, private and public, and competitors and allies are changing. Simply distinguishing between intelligence and non-intelligence issues may prove a major challenge.

To succeed in this fast-paced, complex environment, the Intelligence Community must change significantly. The implications are already apparent. For example, our counterintelligence activities face an array of new and traditional adversaries, yet we must operate within a protected information-sharing environment that challenges existing notions of security and risk.

For collection, the challenge will extend beyond developing a critical source or exploiting a key data stream to determining how to synchronize dissimilar platforms and sources against fleeting and vaguely defined targets, using our collection assets to prompt, detect and respond to what the collection system discovers. **Deep and persistent penetration** is key for collection.

Our analytic professionals will collaborate with world-class experts in academe, commercial interests, and think tanks, all with similar knowledge and personal networks. Deep expertise will require **broad access to open source information**, our unique collection results, and a network of outside experts. Our understanding of the breadth and depth of U.S. policy, intelligence doctrine, and global situational awareness must match the depth of our analyses.

Our most senior intelligence users will place a premium on synthesized presentations that **meld deep expertise with relevance** to the policy agenda and understanding of the nuance of the global situation. Analytic precision and accuracy will be merely the minimum requirements expected by our customers; our analysis must be clear, transparent, objective, and intellectually rich.

Customer demographics and expectations will change; the typical customer in 2015 will be a new generation of government decision-maker, accustomed to instantaneous support, comfortable with technological change, and unfamiliar with intelligence as a privileged source. Such users will expect intelligence to provide customized, interactive support "on demand," and will expect to be treated as a partner – both a source of input and an ultimate intelligence end user.

A Tradition of Evolution & Adaptation

The American intelligence system has long evolved in the face of strategic and technological shifts. Over the first half of the last century, we responded to challenges with advances in aerial imagery, analysis, cryptology, and human intelligence with new organizations like the Federal Bureau of Investigation (FBI) and the Office of Strategic Services (OSS).

During the Cold War, the Intelligence Community fielded high-altitude (e.g., U2/A12), space-based (e.g., Corona), and terrestrial sensors and platforms to peer inside the denied territory of the Communist bloc. The continuing acceleration of change associated with globalization will challenge the Community to respond with innovation once again.

By 2015, a globally networked Intelligence Enterprise will be essential to meet the demands for **greater forethought and improved strategic agility**. The existing agency-centric Intelligence Community must evolve into a true Intelligence Enterprise established on a collaborative foundation of shared services, mission-centric operations, and integrated mission management, all enabled by a smooth flow of people, ideas, and activities across the boundaries of the Intellligence Community agency members. Building such an Enterprise will require the sustained focus of hard-nosed leadership. Services must be shared across the entire spectrum, including information technology, human resources, security, facilities, science and technology, and education and training.


CUSTOMER-DRIVEN INTELLIGENCE
MISSION-FOCUSED OPERATIONS
NET-CENTRIC INFORMATION ENTERPRISE
ENTERPRISE INTEGRATION

1 THE SHIFTING STRATEGIC LANDSCAPE

2 CREATING DECISION ADVANTAGE

Customer-Driven Intelligence
Mission-Focused Operations
Net-Centric Information Enterprise
Enterprise Integration

3 MAKING IT REAL - IMPLEMENTING THE VISION

2 CREATING DECISION ADVANTAGE

To respond effectively to the changing strategic landscape, we need structures, people and systems aligned to ensure a **unified effort**, ready to adapt with greater agility. As we adjust to new challenges and customers, we reaffirm our enduring mission: to provide objective and relevant support to help our customers **achieve decision advantage**.

The Role of Intelligence

Intelligence employs quiet means **to improve our decision-making** while frustrating that of our enemies. We work behind the scenes to inform and facilitate the actions of diplomatic, military, law enforcement, and other customers. We seek to ensure that they know as much as possible about a situation and that their initiatives have the best chance for success. At the same time, intelligence also helps to impair the reliability, speed, and efficacy of adversaries' decision-making.

Although they may be incremental and short-lived, the advantages provided by intelligence may yield significant results — disrupting a terrorist plot, identifying an illicit account, or halting the proliferation of sensitive technology. Intelligence provides a wealth of leads and opportunities that might otherwise be missed. The fragility of such advantages reinforces the need to preserve our sources and methods.

The historical record provides examples of intelligence providing a competitive edge to American and allied decision-makers:

• **Midway, 1942**: American code breakers provided our military forces with a decisive understanding of enemy intentions and capabilities during the darkest days of World War II. Intelligence provided our military commanders the assurance to turn the tables on an intended Japanese naval trap and gain the strategic initiative in the Pacific.

• **Cuban Missile Crisis, 1962**: Imagery intelligence and analysis provided strategic warning of Moscow's dangerous nuclear gambit. The Community provided excellent situational awareness and estimates of possible Soviet responses that greatly assisted the President in navigating a successful outcome from a nearly catastrophic confrontation.

• **The Six-Day War, 1967**: Community all-source analysts correctly forecast the timing, duration, and outcome of the Arab-Israeli crisis. Their pithy, well-reasoned product enabled the President to modulate U.S. involvement and avoid a larger U.S.-Soviet confrontation.

Decision Advantage

Decision advantage results in the ability of the United States to bring instruments of national power to bear in ways that resolve challenges, defuse crises, or deflect emerging threats. Such advantage will not be permanent or absolute.

> *"...the key to intelligence-driven victories may not be the collection of objective 'truth' so much as the gaining of an information edge or competitive advantage over an adversary. Such an advantage can dissolve a decision-maker's quandary and allow him to act. This ability to lubricate choice is the real objective of intelligence."*
>
> *- Jennifer Sims, Director of Intelligence Studies, Georgetown University*

In dealing with future challenges, it is vital to understand how intelligence makes a difference to the decision-maker. The purpose of intelligence is not solely to determine truth, but to enable decision-makers to make better choices in dealing with forces outside their control. Intelligence helps reduce the degree of uncertainty and risk when critical choices are made. Our measure of success is simple: did our service result in a real, measurable advantage to our side?

This approach neatly resolves the potential tension between intelligence objectivity and relevance, often summarized by the axiom that the Intelligence Community "**speaks truth to power**." At times, members of the Intelligence Community have sought to distance themselves from the customer, in order to remain objective; yet such distance could come at a cost in terms of relevance. This is a false choice; **we must be both objective and relevant.** We will do so by acquiring information more crucial to winning, and by denying competitors that same information (e.g., through denial and deception). We will use all facets of intelligence to accomplish this pledge, without confusing

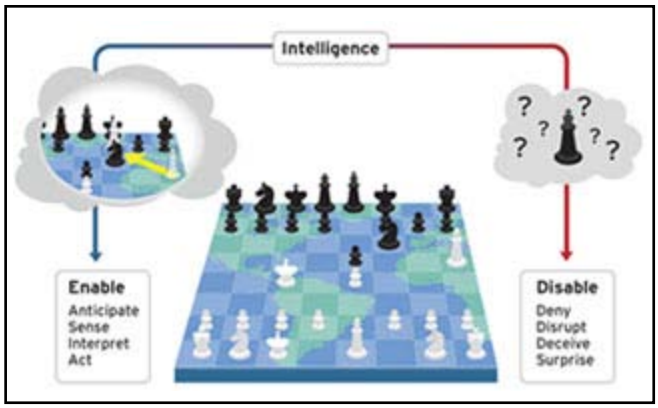


Figure 3: Creating Decision Advantage

the functions with the essentials. For example, some view secrecy as inherent to the intelligence mission. Secrecy, however, is only one technique that may lead to decision advantage; so may speed, relevance, or collaboration. We will not rely on any single, "time-honored" approach in creating decision advantage.

Global Awareness and Strategic Foresight

Another important aspect of decision advantage lies in preparing our decision-makers for **strategic surprises** — those forces or issues that lie off the decision-maker's agenda but may emerge to challenge our intended outcomes. The ability to anticipate change — recognizing key early indicators and alerting decision-makers — is a key role of intelligence. While our capabilities to monitor already-known threats are well-honed — with mission managers generally assigned to oversee our handling of top-tier threats — adaptive intelligence also requires strategic capabilities for sensing and evaluating "weak signals" and other indicators of emerging issues and security risks. The need to prevent strategic surprise was one of the prime factors in the genesis of the U.S. Intelligence Community in 1947. America's rise to superpower status, combined with the complexity and interconnectedness of the emerging strategic landscape, demand that our Intelligence Enterprise provide global awareness and strategic foresight.

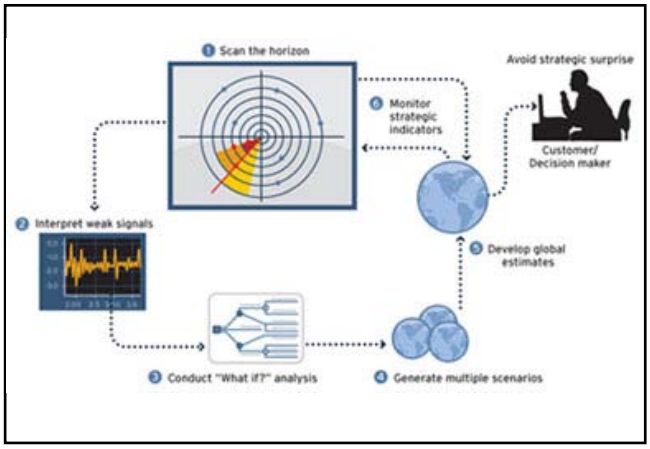


Figure 4: Global Awareness and Strategic Foresight

Strategic warning and predictive estimates were standard art forms in the less dynamic Cold War period. Our anticipated strategic environment models closely on chaos theory: initial conditions are key, trends are nonlinear, and challenges emerge suddenly due to unpredictable systems behavior. In this environment, one prerequisite for decision advantage is **global awareness**: the ability to develop, digest, and manipulate vast and disparate data streams about the world as it is today. Another requirement is **strategic foresight**: the ability to probe existing conditions and use the responses to consider alternative hypotheses and scenarios, and determine linkages and possibilities. We believe our customers will seek our inputs on what may surprise them, if we are capable of placing such inputs in a larger context and demonstrating rigor in our analytic approaches to complexity.

To carry out its mission in an increasingly turbulent and complex global environment, the Intelligence Enterprise must enhance capabilities to evaluate global risks affecting our national security. Greater systems interconnectedness increases the need to identify **vulnerabilities emerging at the nexus of multiple systems** (e.g., critical information infrastructures, disruptions in energy supplies, fragile financial markets, and climate change-related spread of diseases) and the potential for multiple, simultaneous crises. Global awareness and strategic foresight will provide the response to these challenges, linking methods for strategic forecasting and assessment of systems vulnerabilities in constantly renewed communities of diverse expertise and insight. As much of this expertise will be outside of the Intelligence Community, our efforts will be **done in partnership with business, academic, other government, and non-government sectors**.

Customer-Driven Intelligence

By 2015, the Intelligence Community will be expected to provide more details about more issues to more customers. We anticipate different types of customers — with greater expectations — and new demands to change the basic engagement model by which we serve them.

Although there is no typical customer, we will be providing intelligence to a computer-literate generation that grew up with the Internet and user-generated content (e.g., YouTube, blogs, wikis), in which they acted as both a consumer and contributor of information in an "on-demand" environment.

As a consequence, customers in 2015 will define their relationships with the Intelligence Enterprise differently — shifting focus from today's product-centric model toward a **more interactive model** that blurs the distinction between producer and consumer. To create and sustain deep partnerships, the Intelligence Community will require greater use of liaisons who can build relationships and leverage networks to connect information, expertise, and needs in a fluid environment. We will also need to exploit commercial technologies to develop new ways of providing service.

Not only will the type of customer change within our existing federal policy-making sets, but the range of customers will broaden to emphasize other federal departments (e.g., Health and Human Services, Agriculture, Commerce), state and local agencies, international organizations, and private sector and non-governmental organizations.

Generation Y Mindset for 2015

- *Born around 1980; they have no meaningful recollection of the Reagan era or the Cold War.*
- *"Digital natives" who have owned a cell phone their entire adult lives.*
- *Always received most of their news from the internet.*
- *Sept 11, 2001 dramatically changed their college experience.*
- *Comfortable multi-tasking and working in teams.*
- *Currently in the third career (not job).*
- *Telecommuting is a way of life, not an agency initiative.*
- *Savvy in rapidly accessing and evaluating public domain knowledge.*

Tailored Support

Not all customers will expect the same level of interaction with our Intelligence Enterprise. Our approach to providing customers with tailored support resulting in decision advantage will span a spectrum of customer types, **from partners to clients to consumers**. Our partners will demand the most intense, personalized support and desire to be actively engaged with us while jointly coming to conclusions. Partners will seek to provide us with their expertise, access to their networks, or feedback from their actions and policies. Clients will prefer a more consultative role: close and sustained interaction focused on outcomes relevant to their agenda. Consumers will accept a more transactional relationship with the Enterprise; they will ask questions and expect quick, straightforward answers. One common theme among all of our customers will be a growing substantive and technological sophistication.

Customer Relationships

The importance of the customer in the future clearly calls the Intelligence Community to apply best practices in customer support. To engage customers effectively, we must use sophisticated techniques to elicit their needs and to evaluate our performance. Rather than asking customers, "What are your intelligence priorities?," we will engage them with, "What do you want to accomplish?" Intelligence support to customers will become more of a relationship than an event.

We will begin by extending the lessons learned from our own successful customer support activities (e.g., the President's Daily Brief). We must offer customer service at many levels (not just for the most senior customers) and monitor our progress to inform future changes. We must build an approach that exposes our intelligence professionals to customers and familiarizes new customers with our capabilities and limitations. Key to this will be development of a customer engagement and management model that assigns "**channel managers**" to support specific customers, and apportionment of the channel management function by customer type, by functional topic, or by other means.

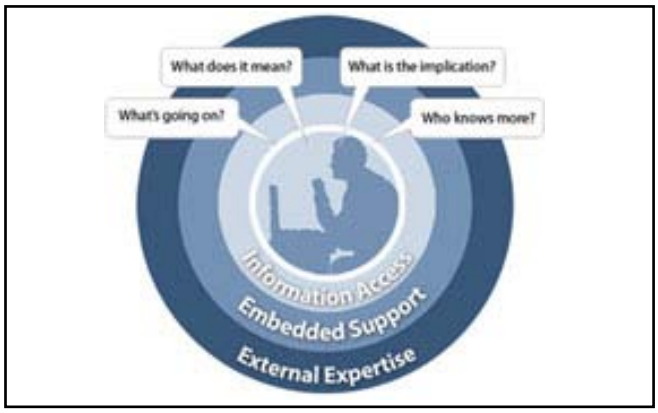


Figure 5: Customer-Driven Intelligence

Our analytic products will increasingly resemble **customized services**, with an emphasis on maximum utility rather than simple releasability. Under concepts such as effects-based analysis, we will engage customers with "What if?" considerations in addition to "What?" conclusions. To do so, our analysts will leverage disparate data and analytic tools and services, working in mission-focused distributed analytic networks.

We also anticipate a growing public demand for intelligence. Most intelligence work will remain classified and limited in distribution to ensure it produces the desired decision advantage for our U.S. government clients. However, the Intelligence Community must adapt to the growing requirement for its analysis to inform the American public.

Although the customer sets, expectations, and engagement models will change, the Intelligence Community will still be expected to provide objective, relevant, and timely intelligence to give our customers a sustained decision advantage in support of our national security objectives.

Mission-Focused Operations

In the past, the Intelligence Community was siloed into discrete disciplines (e.g., signals intelligence, human intelligence, geospatial intelligence, counterintelligence) and functions (e.g., tasking, collection, analysis, dissemination). These silos often led to competition and duplication. Although the agency-centric operating model worked well during the Cold War, it cannot succeed in the current environment, which changes rapidly. We need a mission-focused operating model that is agile, lean, and flexible enough to respond to a dynamic environment. Our new operating model must adapt our enduring roles to our new challenges, incorporate new technologies and processes, and build on our initial successes at integration and collaboration. On the one hand, we

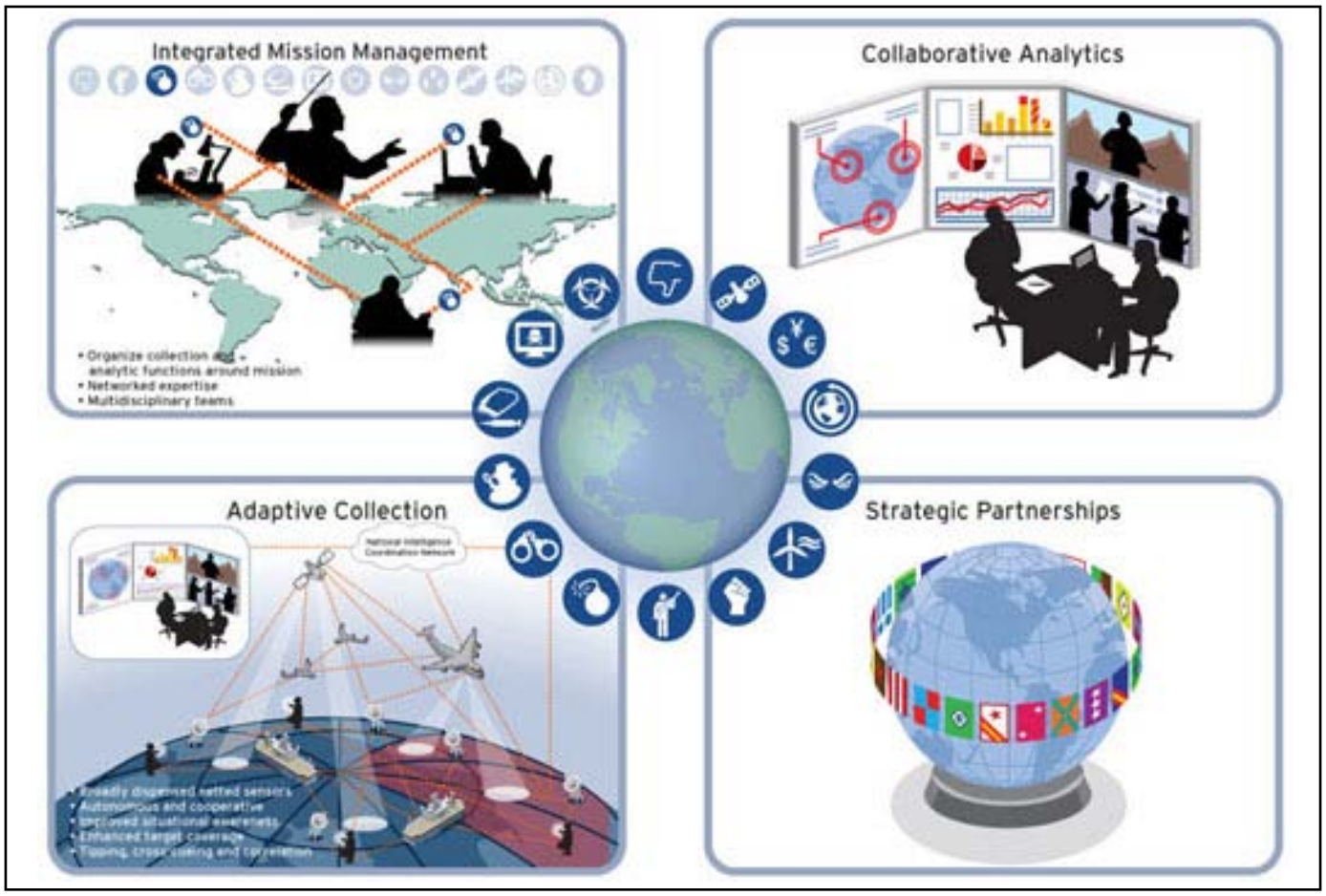


Figure 6: Mission-Focused Operations

must maintain excellence in separate disciplines; on the other, we must develop greater functional integration. More specifically, we must transcend the current agency-based linear model — task, collect, process, exploit, and disseminate — and develop a more mission-based model that is fluid, synchronizes collection, collaborates on analytic issues in real time, and broadens our partnership strategy.

Accordingly, this **integrated operating** model will transform the traditional intelligence cycle into a more dynamic series of interactions among four key operating principles: Integrated Mission Management; Adaptive Collection; Collaborative Analytics; and Strategic Partnerships. This model is designed to promote accuracy, speed and agility without the constraints of organizational equities or functional stovepipes. This new operating model has a simple objective: to operationalize the Intelligence Enterprise, raising mission focus from the unit or agency-level up to a Community-wide activity. To this end, we will need to clarify roles and responsibilities, streamline decision rights, and establish Enterprise-wide governance to enable this new operating model. When this objective has been realized, the Intelligence Enterprise will be both agile and capable, and our partner-customers will benefit from an intelligence-based decision advantage.

Integrated Mission Management

With some exceptions, the current structure and operation of the Intelligence Community are oriented toward agencies, disciplines and specific functions rather than around priority missions. To respond to the dynamic and complex threat environment of the 21st century, our operating model must emphasize **mission integration** – a networked knowledge-sharing model that rapidly pulls together dispersed and diverse expertise and resources against specific missions. This model could manifest itself through an array of networking options – national intelligence centers, mission managers, task forces, and communities of interest.

Integrated Mission Management will improve collection and analysis speed by reducing vertical levels and clarifying tasking authority; enhance innovation through diversity and cross-pollination of ideas; ensure completeness by leveraging niche expertise; and reduce duplication through better coordination. Mission managers will oversee all aspects of national intelligence related to their mission areas and serve as the customer interface for their respective mission responsibilities. Historically, the Community has employed **mission-focused opera-**

Figure 7: Integrated Mission Management

tions as a best practice for forward-deployed intelligence support. The time has come to import this "lesson learned" back to our stateside organizations and activities. Doing so will require **resolute leadership**, since it will entail a **dramatic reconceptualization of how we organize, train, and operate.**

Adaptive Collection

To overcome uncertainty, the collection community will have to "hedge its bets" about future targets and technologies, and adapt quickly to challenges and opportunities; reaction time will be the key to success. The elusive, transitory nature of our targets, and the imbalance between the increasing demand for information and the capacity of our means to collect it, **require multiple, integrated collection systems**. Each of the collection disciplines — human intelligence, signals intelligence, computer network exploitation, geospatial intelligence, measurements and signatures intelligence, open source intelligence, acoustic intelligence, and foreign materiel acquisition — will continue to play key roles, although their relative importance will almost certainly change over time. Our future success demands integration of collection capabilities at all levels.

The principle of Adaptive Collection emphasizes the dynamic allocation and re-allocation of collection, processing, and exploitation. It also provides a mandate to prioritize between open and secret collection means, since secret sources and methods must be reserved for use against those targets that cannot be penetrated using other, more efficient (i.e., open source) means. No aspect of collection requires greater consideration, or holds more promise, than open source information; transformation of our approach to open sources is critical to the future success of Adaptive Collection.

Adaptive Collection is built on a global collection network comprising many netted sensors that can work autonomously- and cooperatively in near-real time. Collection assets would move into and out of specific areas of interest, using already collected information to inform their activities, and in turn, focusing on collecting only that which cannot be obtained by other means. These assets would both push and pull data — raw, semi-processed, and final — into and from our information technology backbone network. The collected data will belong to the Intelligence Enterprise; no single agency "owns" its collection take. We would improve situational awareness, reduce collection time, enhance target coverage, increase robustness of collection capability, and sharpen accuracy through cross-cueing and correlation.

Above all else, the collection community will be measured against its ability to achieve deep and persistent penetrations that are key to understanding foreign leaders' intentions, foreign nuclear programs, terrorist groups, and proliferation networks. Second, there will be more emphasis on multi-agency teams pursuing "multi-INT" collection strategies. Third, we envision a collection community comprising people who speak the languages and know the cultures in which we must operate. Fourth, we envision a collection community capable of rapidly fielding technological innovations that obtain needed information. Finally, we envision a collection community with a **fully integrated processing, exploitation, and dissemination architecture** that moves information quickly to its users. Such architecture will feature both automated and "user-in-the-loop" collection and processing. It will also entail modernization of the collection enterprise to facilitate a holistic awareness of sensor status, tasking and alignment of all collection systems to better respond to its customers. Above all else is the demand that the information reach those who need it, when they need it, in a form that they can easily absorb.

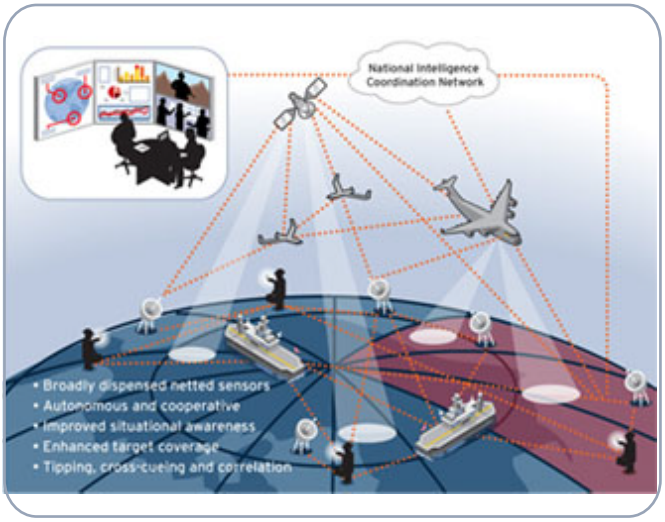


Figure 8: Adaptive Collection

Collaborative Analytics

The analytic community will be expected to understand and develop judgments on a broad spectrum of national security threats, support a more diverse customer set, and cope with access to unprecedented amounts and types of information. Information overload already presents a profound challenge to our business model. Given these challenges, the analytic community has no choice but to pursue major breakthroughs in capability. Applying the principle of Collaborative Analytics, analysts will be freed to work in a fundamentally different way — **in distributed networks focused on a common mission**.

Analytic organizations will therefore make a dramatic shift from traditional emphasis on self-reliance toward more collaborative operations — a shift that will allow the Community as a whole to perform routinely at levels unachievable in the past. Analysts will act individually and as members of Community teams — addressing customer queries, driving collection, trying new methodologies, and collectively building corporate knowledge. The focus of their collaboration will shift away from coordination of draft products toward regular discussion of data and hypotheses, early in the research phase. Collaboration will be aided by expertise registries updated automatically. Managers will use these registries with smart networks to disseminate customer requests directly to the Community analysts best able to contribute. Analysts who offer to join in a response will be directed to a collaborative work site ready to support them.

Information overload will be averted through sophisticated data preparation and tools. In 2015, new information will be tagged so tools can trace related data across our holdings. Analysts will use such tools to mine the data, to test hypotheses and to suggest correlations. Analysts will routinely employ advanced analytic techniques, including scenario-based analysis, alternative analysis, and systems thinking. The move toward extensive use of data, tools, and modeling is at the heart of collaborative analytics.

Collaboration in analysis will also foster smarter collection. The Library of National Intelligence and shared postings of ongoing research will continuously record what we know — and this will help avoid unnecessary new collection. In 2015, the library will hold half a decade of disseminated intelligence, where analysts can discover all available reports — granting immediate access if they are cleared and offering guidance on next steps if they are not. Analyst proposals for new collection will be posted for collaborative review. Collectors will mine that data to improve their own collection planning. Many collectors will share large amounts of newly collected data, tagged for easy discovery and linking, in secure environments with analysts. Bringing analysts and collectors closer together will promote deeper knowledge of collection across the analytic community, which will further improve both the quality of collection requests and the sophistication of analytic judgments.

As analysis becomes more integrated, collaborative efforts will emerge to serve our customers. Our products and services will change to meet evolving needs for timely information and insight, delivered in ways that are personalized. Demand will vary from one client to the next, including virtual meetings, models and simulations, mobile access, and user-selectable versions at different classification levels. New breakthroughs will be driven by timely corporate sharing of information about the needs of key clients, plans for meeting those needs, actual intelligence provided, and feedback received.

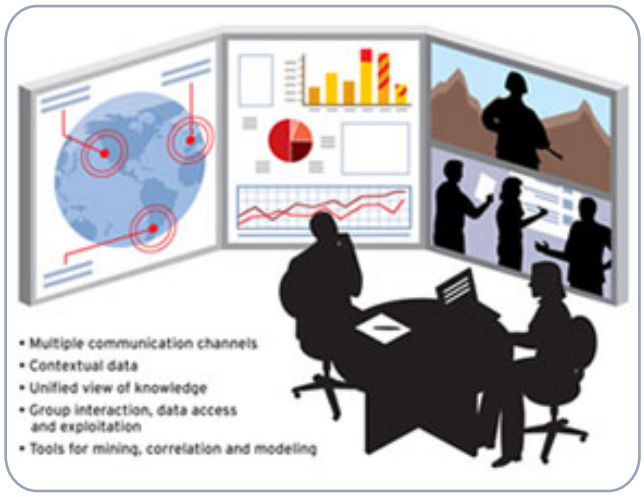


Figure 9: Collaborative Analytics

Without obscuring critical disagreements, the Community will free customers from the burden of doing their own intelligence comparison, integration, and deconfliction. Close ties between an integrated analytic community and its customers will allow real-time engagement and clarification of customer needs. By 2015, we will track Community performance against priority topics in a standardized fashion. Managers will be able to see the impact of local contributions to overall Community support to key customers, and will use this information to drive continual improvement and **rapid adaptation** to changing customer needs.

Strategic Partnerships

Given the broad spectrum of threats, looming budget constraints, and the need for deep analytic expertise, the Intelligence Enterprise will have to expand its network beyond the boundary of the traditional Intelligence Community. The global nature of intelligence makes it imperative that we continue to seek opportunities to collaborate with our allies and foreign partners. Our strategic partnerships will

Figure 10: Strategic Partnerships

include traditional international allies, opportunistic partners, multinational organizations, civil societies, academe, and industry.

The U.S. Intelligence Enterprise clearly benefits through **increased global coverage, local expertise, and improved synergies**. These benefits span the entire partnership spectrum, depending on the breadth and depth of the relationship: historical bilateral partnerships, alliances, joint programs, transactional, and ad hoc. To reach their full potential, strategic partnerships will need Community-wide strategies and policies, strong relationship managers and liaisons, and a flexible and secure information-sharing environment. Our partnerships are based on a series of personal relationships reinforced by policy and process. While we must have oversight into the full range of our partnership activities, their success ultimately comes down to the flexibility and effectiveness of those representing us in the relationship. Our representatives must be empowered to engage in the relationship with a strong understanding of the overall "commander's intent" of our activities.

Net-Centric Information Enterprise

Information — classified and open source — is the fuel that powers intelligence. Sharing products is no longer adequate; collectors and analysts have the responsibility to provide much more of what they produce beyond final reports. As a consequence, the Intelligence Enterprise must be built on a robust information infrastructure, based on a culture of information sharing and supported by a range of common services that allow the analytic end user to transform the **deluge of data** into predictive, actionable intelligence.

The end state will be **seamless access** to all intelligence information, tools and processes across multiple agencies and databases. Our information architecture will have to undergo a fundamental shift: from the multiple hub-and-spoke model of information collection, analysis, and dissemination based on specific discipline to a **unified architecture** designed around a common "cloud" (i.e., a distributed peering network) containing our information. This information infrastructure will allow authorized end-users to discover, access, and exploit data through a range of services, from federated query to integrated analytic tool suites.

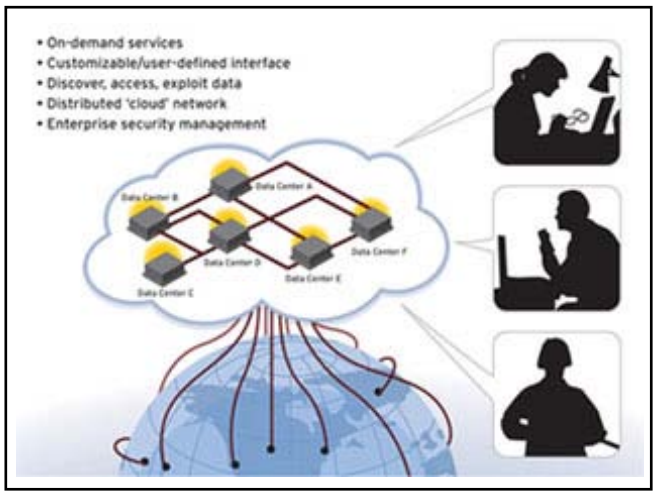


Figure 11: Net-Centric Information Enterprise

Common Information Infrastructure

Currently, each intelligence agency operates and maintains its own network and information infrastructure: power, cooling, circuits, switches, routers, databases, information management systems, data centers, security and enterprise systems management tools. By 2015, we will migrate to a common "cloud" based on a single backbone network and clusters of computers in scalable, distributed centers where data is stored, processed, and managed. The shared data centers will be unique facilities designed and located for access to communication and power supplies. The Intelligence Enterprise will benefit greatly from a more robust, secure, and effective means to organize, update and retrieve all of the information it collects. The centers will also allow experience and technologies employed across the Community to be leveraged, focusing scarce technical resources and reducing costs.

On-Demand Services

Over the last 20 years, the Intelligence Community has been challenged to keep pace with rapidly evolving information technology. Although a less-than-agile acquisition and procurement system has been part of the problem, the Intelligence Community is also undermined by its basic approach. If we are to maintain a technology edge, we must adopt an enterprise-wide, **service-oriented architecture** that is interoperable with systems in other federal departments, and can share information with non-traditional partners. A service-oriented architec-

ture provides a proven means to adapt new technologies while responding to changing user needs. By creating "software as a service," this architecture reduces system complexity and deployment risks through a shared development style, uniform standards, and common interfaces. These services will enable a user-defined analytic environment through the use of **composite applications** – discrete services that can be pulled from a central library and dropped into a user-defined workspace.

The range of Enterprise-wide services that should be deployed by 2015 include communication services (e.g., common e-mail, directories, calendaring, and collaboration); data services (e.g., federated queries and searches, tagging, entity extraction, and storage); security services (e.g., single sign-on, access control, monitoring, and auditing); and analytic services (e.g.,portals, data mining, visualization, and modeling and simulation tools).

Enterprise Integration

Providing our customers with a decision advantage and collaborating around our core mission areas require a **strong foundation** that integrates the vital components of the Intelligence Enterprise — people, processes, and technology. Historically, organizational differences — competing cultures, non-interoperable systems, unclear decision rights, and conflicting business rules — acted as barriers to collaboration, greatly undermining our ability to adapt and reducing our organizational agility. Although we have progressed since the 9/11 attacks, and significant initiatives are under way, we will need **continued leadership and organizational commitment** to truly integrate the Intelligence Enterprise by 2015.

Figure 12: Enterprise Integration

Human Capital and Knowledge Management

At the core of the Intelligence Enterprise in 2015 are our people. One of our biggest challenges will be the ability to attract, train, and retain a highly skilled, innovative and adaptive workforce. The intelligence workforce of the future will be more distributed, virtual, and flexible than at anytime in the past; the implications for our information technology infrastructure and facilities are significant. We need professionals with strong linguistic skills, deep cultural understanding, and mastery of the "human terrain." **Cultural, linguistic, and technical diversity** will be critical to the workforce of the future. Moreover, the changing strategic environment will require a **more entrepreneurial** and customer-focused workforce that can combine deep functional knowledge and expertise with broad networking and collaboration skills. Strict boundaries, such as the distinction between collectors and analysts, must become permeable divisions that highlight different roles our intelligence professionals play during an intelligence career, not exclusive memberships.

Echo of the Future: Joint Duty

In 2007, with the support of the leaders of the six affected US government departments, the DNI signed the Joint Duty policy guidance, making joint duty a prerequisite for promotion to senior executive within the Community. This policy sets a firm standard that -- for the first time -- rewards Enterprise-minded culture

Our leaders will need to transcend the traditional independent, agency-centric orientation, and move toward a leadership style based on cross-agency collaboration and interdisciplinary experience. In particular, this will require **leadership** that can build coalitions across agencies and cultures, bound by a shared purpose and unity of action to achieve mission objectives. Managers will adopt a new role more focused on professional development and measuring work unit quality, less focused on product oversight and review. We will need leadership development programs, performance evaluation systems, and an **incentive structure** that span the Intelligence Enterprise.

By 2015, the focus should shift from information sharing (e.g., interoperable systems, information discovery and access) to knowledge sharing (e.g., capturing and disseminating both explicit and tacit knowledge). Just as we are dismantling today's information "silos," we will need to bridge the knowledge "archipelagos" of tomorrow in a systematic way that combines both content and context in an on-demand environment. Robust social networking capabilities will be required — expertise location, ubiquitous collaboration services,

integrated e-learning solutions, visualization tools, and enterprise content management systems. More importantly, a strategic approach to knowledge sharing and management must be incorporated that includes lessons learned and concept and doctrine development.

Modern Business Practices

The Intelligence Community cannot depend on ever-increasing budgets to develop leading-edge technologies, field new capabilities and run current operations. We have to adopt modern business practices that will make us more effective, efficient, nimble, and **accountable**. The current business model is burdened by archaic rules, fragmented practices, and non-interoperable business systems. If we are to optimize our limited resources, we must transform the model; our procedures and systems for planning, programming, **budgeting** and managing personnel **security** must fundamentally change.

Business System Modernization
A key enabler of organizational adaptability and operational agility is an integrated planning, programming, budgeting, enterprise management, and finance system that links and **aligns strategy to budget, budget to capabilities, and capabilities to performance**. We need processes and systems that allow us to anticipate the future for long-term planning, programming and budgeting, and also enable us to respond rapidly to time-critical issues. An integrated business management system must support these business processes. Senior managers must receive timely, accurate and reliable financial and performance information. We must have simple, reliable performance criteria and metrics that demonstrate progress toward our goals.

As part of business modernization, we will move toward a **core financial system** that integrates budget and performance data, while standardizing and streamlining common business processes (e.g., procurement, travel, acquisition, human resources). This will allow us to employ business analytics to drive evidence-based decision-making and more effectively manage our resources.

Security Transformation
By 2015, the security function within the Enterprise will be transformed while growing in importance. Our security practices must parallel, in pace and direction, our technology and workforce efforts. Personnel security must transition from a barrier approach to a **full lifecycle approach**. A web of personal, information technology, and physical security measures will ensure all professionals maintain the highest security standards across an intelligence career. The security officer of the future will be analytically trained and technologically adept, capable of adapting broad security policy to constantly changing technological or customer demands. The Intelligence Enterprise will function on common security standards to empower continuous monitoring. The demands of knowledge sharing with strategic partners will push the security function into a new role: determining classification, and monitoring and governing the overall development of classified information. Security professionals will become primarily responsible for ensuring that our "secrets" are truly secret — and remain so. This new role for security will demand a radical simplification of the classification system and its many codewords and caveats. In the end, the foundation for classification will remain the potential for damage to our nation's security.

Agile Infrastructure
By 2015, employees from different agencies will have to be collocated to more remote locations, away from centralized headquarters. The needs for cross-organizational collaboration, cross-functional teams and programs such as Joint Duty will require a more agile infrastructure. By this, we mean to suggest a deliberate strategy that shifts from agency-centric, massively consolidated facilities towards a more distributed and integrated model that uses **hoteling practices** and creates more **open** and collaborative **workspaces**. Agile infrastructure will be based on two principles — **collocation** of cross-functional teams (e.g., collection disciplines, science and technology, analysts, mission managers) around projects or specific missions, and **virtual collocation**, where a dispersed workforce can rapidly coalesce to respond to new tasking. A facilities strategy will be developed that takes into account both physical and virtual collaboration; a common badging and credentialing system will be required to allow the intelligence workforce to move seamlessly among facilities.

Innovation, Science and Technology

Most of the technology base comes from the private sector; technology cycle times are decreasing, and technological innovation has its source in many countries. Thus, the Intelligence Community will need to fundamentally reconceptualize and redesign our acquisition and procurement policies and processes to emphasize adaptation, speed, and agility. Moreover, since services are a large and increasing portion of the budget, we require procurement policies and practices that acquire capabilities, not simply buy "hours." Innovative, performance-based acquisition solutions will be required. These solutions must reward innovation, performance and risk-taking from our partners in the private sector.

Although we will continue to rely on commercial best-of-breed technologies and best practices, the Intelligence Community will still need to research, develop and field disruptive technologies to maintain a competitive advantage over our adversaries. We cannot evolve into the next technology "S curve" incrementally; we need a revolutionary approach. Breakthrough innovation, disruptive technologies, and rapid transition to end-users

will be required, as well as a high tolerance for risk and failure. We need to encourage and reward risk-taking, creativity, and entrepreneurial behavior both with our government employees and our private sector partners. We will need to leverage organizational options (e.g., creating an Intelligence Community version of the Lockheed model Skunk Works®) as well as process improvements (e.g., leveraging workforce diversity to improve cognitive diversity) to foster the creativity we seek. We must work closely with our congressional oversight colleagues to enable an innovation-friendly culture.

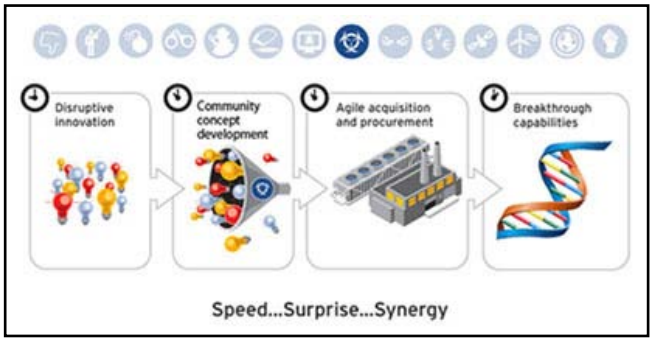


Figure 13: Innovation, Science and Technology

Creating a culture of innovation will require greater focus on advanced concepts, technology, and doctrine to enhance leadership, organizational alignment and resources. We need to establish a mechanism that allows us to continuously survey the future, capture potential mission impacts, and develop and experiment with new integrative intelligence concepts and technologies.


VISION
2075
2014
2013
2012
2011
2010
2009

1 THE SHIFTING STRATEGIC LANDSCAPE

2 CREATING DECISION ADVANTAGE

3 MAKING IT REAL - IMPLEMENTING THE VISION

THE WAY AHEAD
KEY DESIGN CONCEPTS
STRATEGIC ROADMAP
MANAGING CHANGE

3 MAKING IT REAL – IMPLEMENTING THE VISION

"It is not the strongest of the species that survives, nor the most intelligent, but the one most responsive to change."
- Charles Darwin

The Intelligence Community of today is composed of some of the most dedicated and capable public servants, and they continue to advance the intelligence reform agenda. However, our efforts to incrementally improve the existing operating model and capabilities will be insufficient in the rapidly evolving, dynamic environment we have entered.

Our many improvements since 2001 have been fueled by sorely needed additional resources, but anticipated budget pressures will likely end this largess in the future. We cannot afford to retreat into incremental improvements or simple efficiencies, which will cause us to fall further behind. We have **no choice but to transform** our profession along the lines presented in our new operating model.

The Way Ahead

Our national security institutions have demonstrated a tendency to focus on their areas of authority and expertise while proving less able to organize joint efforts that fall between domains. The Intelligence Community has suffered the consequences of this problem and perpetuates it. As we learn to unify all instruments of national power in truly joint, interagency initiatives, we will find that intelligence only grows in importance for the new players on the national security team.

The National Intelligence Strategy of October 2005 proclaimed a vision of our Community as "a unified enterprise of innovative intelligence professionals…," but it did not further define that end state. Vision 2015 outlines the rationale for becoming an enterprise, and details the differences in our new operating model. Our Intelligence Enterprise will advance along the distinct paths of adaptability, alignment, and agility.

Key Design Principles

To succeed in this new environment, the Intelligence Community must undertake fundamental organizational and cultural change, moving from a bureaucratic command-and-control model to an integrated, collaborative, networked Enterprise. As we build this Intelligence Enterprise, we need to adhere to a few simple design principles — adaptability, alignment, and agility.

Adaptability is an organization's aptitude for anticipating, sensing, and responding successfully to changes in the environment. It is a process that requires us to continuously survey the external environment, identify discontinuous threats or opportunities, understand the gaps between challenges and capabilities, experiment with new ideas, and learn from experience. The keys to adaptability are active engagement and an openness to outside ideas and influences.

Alignment is the degree of consistency and coherence among an institution's core strategy, systems, processes, and communications. Alignment occurs within a context of strategic direction, ensuring our activities are prioritized to realize a specific vision, without predetermining "how" the vision will be accomplished. It is a control mechanism ensuring that strategic goals, objectives, deployed capabilities, and organizational performance are clearly linked and focused on mission achievement. The key challenge to achieving alignment is ensuring unity of effort without succumbing to conformity of thought.

Agility is an organization's ability to reconfigure processes and structures quickly — with minimal effort and resources — to seize opportunities and address strategic risks. In a complex, dynamic environment, no amount of forecasting can predict every change. We need to create an organization that responds with speed and precision to unforeseen events. Agile organizations possess flexible, modular design, shared infrastructure, and an innovative, risk-tolerant culture.

These design principles need to be integrated and reinforced. Adaptability without alignment creates chaos and wastes resources on duplicate and conflicting efforts; adaptability without agility results in an organization that can "see the train coming down the tracks" but cannot get out of its way. We must ensure that our new organizational models and intelligence concepts adhere to these design principles.

Strategic Roadmap

The Community needs a detailed plan to enact this vision and become an Intelligence Enterprise. The Director of National Intelligence will establish a senior-level design team to develop the specific actions and milestones comprising a roadmap to accomplish our vision. The roadmap will detail actions that will ensure our strategic adaptability, enhance alignment, and improve our organizational agility.

Adaptability actions:

- Develop the means to **forecast** the future environment, anticipate future threats and missions, and consider and deploy innovative alternate intelligence capabilities.
- Develop and experiment with new operational concepts and tactics in support of the integrated operating model.
- Align **innovation** and **experimentation** efforts (e.g., Galileo) in support of this effort.
- Implement and examine multiple models of **mission management** to determine how to best use them operationally.
- Build the organic capability to conduct **exercises** and modeling and simulations throughout our processes (e.g.,analytics, collection, mission management, etc.) to innovate and test new concepts and technologies.
- Integrate lessons learned, history, and education and training activities (as appropriate) to establish the basis for **learning from our successes and failures**.
- Exploit best practices in customer engagement to establish Enterprise-wide **channel managers** who actively engage with our developing partner-customers and evolve our engagement model.
- Establish an intellectual "home" for intelligence professionalism, linked to the **National Intelligence University**, to serve as the thought leader for the Enterprise.

Alignment actions:

- Re-image the Community to acknowledge that member relationships to the Office of the Director of National Intelligence differ. Formalize these different relationships in **policy**.
- Develop an Intelligence Enterprise strategy that **aligns ends, ways, and means**.
- Deploy a unitary, transparent, and disciplined **strategic management process** to drive integrated strategy-to-capabilities-to-plans and budgets across the enterprise.
- Build an annual strategy-to-plans structure that focuses agency and element performance on specific goals and objectives, with tangible **metrics**, to ensure that we progress toward accomplishing our missions and achieving our vision.
- Integrate our **counterintelligence** capabilities through increasingly rigorous policy, doctrine, standards and technology, and align counterintelligence with our broader National Intelligence Strategy goals and objectives.
- Develop the policies, procedures and infrastructure to permit the creation of new, temporary, **mission-focused** elements to serve as the operational arms of the Intelligence Enterprise.
- Embrace a **culture of performance** that encompasses the individual, the agency and the Enterprise.

Agility actions:

- Re-image the Intelligence Enterprise to find ways to flatten the hierarchy and reduce to the "tooth-to-tail" ratio.
- Create an Intelligence Enterprise concept of operations to detail the components of the integrated operating model.
- Clarify roles, missions, functions and decision rights through policies and procedures and streamlined processes.
- **Dramatically improve the access and flow of critical information** — both operational and management — across the Enterprise.
- Shift from large, expensive collection platforms towards smaller, netted collection systems.
- **Identify and consolidate services of common concern** (e.g., human resources, finance, public affairs, general counsel, legislative affairs) to streamline and simplify Enterprise support activities.
- Seek new means to enhance enterprise culture through integrated operations (multi-agency), practices (doctrine, tradecraft, etc.) and support services (alternate work locations, hoteling). Deploy such capabilities in parallel with existing ones and rigorously pursue the better performing options.
- Foster a risk-tolerant culture by rewarding agencies, leaders, or other intelligence professionals who seek to adopt new practices to improve performance or efficiency.

Leading Change

The first and most significant impediment to implementation is internal and **cultural**: we are challenging an operating model of this Vision that worked, and proponents of that model will resist change on the basis that it is unnecessary, risky, or faddish. These opponents will posit that incremental change is working, the environment is not really that different, and the new methods are unproven.

A second impediment is existing institutional barriers, which create **friction**. Few things sap the determination for change as effectively as the friction induced by layers of bureaucratic inefficiency working to frustrate any endeavor. Stove-piped "back-office" functions that make even simple personnel or operational activities difficult will complicate nearly every aspect of transformation.

A third impediment is **budgetary**. Dramatic transformation of the Intelligence Community will require stable and somewhat predictable budgets. While some efficiency gains will be realized through rationalization and consolidation, change cannot happen on the cheap. This challenge must first be addressed by responsible internal management practices at all levels, guided by a detailed strategic roadmap and better communications and engagement with the appropriators and authorizers.

A fourth impediment is environmental: the **tyranny of the immediate.** For nearly four decades, intelligence reform has remained largely stymied by the inability of the Community to emphasize sustained implementation. Senior leaders across the Intelligence Community face constant pressure to depart from carefully considered approaches to deal with pressing day-to-day challenges.

Translating our Vision into reality will take more than desire and good intentions. First, we will need effective outreach and aligned communications to energize the organizations that comprise the Intelligence Enterprise. We will need strong leadership, unyielding commitment, and empowered change agents to mobilize the workforce. Second, we must align the Enterprise through a new National Intelligence Strategy, a strategic roadmap that establishes key capability milestones over the FY11-16 planning and programming horizon, and the development and management of annual implementation plans to ensure accountability and progress, Third, we will need to assign responsibility for accomplishing this Vision to key areas throughout the Enterprise: missions (e.g., counterterrorism, counterproliferation, counterintelligence, etc.), agencies, program managers, and functional leads (e.g., Chief Information Officer, Chief Human Capital Officer, Science and Technology). Fourth, we need to institutionalize change by ensuring short-term wins, measuring and rewarding performance against the vision, and ensuring continuous improvement through quarterly reporting and evaluation sessions with senior leadership throughout the Intelligence Enterprise. Perhaps most importantly, senior leadership must commit to building a culture that will take risk to make this Vision real.

The transformation of the Intelligence Community into an Intelligence Enterprise will not come easily; if it were an easy process, our dedicated intelligence professionals would have completed it long ago. Although change is disconcerting by its very nature, the changes elaborated in this Vision are necessary for our continued success and for the defense of our nation. We will encounter halting progress and occasional setbacks, but we will succeed in remaking today's best Intelligence Community into the best Intelligence Enterprise the world has ever seen.

Figure 14: Leadership Driving Transformation

VISION 2015 At-A-Glance

Decision Advantage

The employment of all facets of intelligence to acquire and provide information to gain an edge or competitive advantage that is crucial to winning while denying competitors that same information

Customer-Driven Intelligence

The ability to broaden the customer set while deepening relationships to drive the development and delivery of objective, relevant, timely, and accurate intelligence through a range of tailored products and services

Global Awareness and Strategic Foresight

The ability to anticipate, and alert decision-makers to strategic surprises by sensing and evaluating weak signals and developing alternative hypotheses and a range of scenarios to better understand a complex, rapidly evolving and unpredictable global environment

Mission-Focused Operations

A concept of operations that transcends the current agency-centric model towards a more mission-based configuration that is agile, synchronizes collection, and connects dispersed and divergent expertise to collaborate on hard problems

- **Integrated Mission Management** - Integrates and orchestrates resources and expertise around mission, not agency or discipline
- **Adaptive Collection** - The dynamic reallocation of distributed and networked sensors that can work autonomously and cooperatively to improve situational awareness, reduce collection times, enhance coverage, and improve accuracy through cross-cueing and correlation
- **Collaborative Analytics** - The capability to manage and exploit unprecedented information overload and free analysts to work in distributed information networks focused on a common mission
- **Strategic Partnerships** - The ability to extend the Intelligence Community beyond the traditional network to increase global coverage, deepen local expertise, and capture mission synergies by expanding our partnership model to include allies, opportunistic partners, academe, and industry

Net-Centric Information Enterprise

A common information infrastructure that provides seamless access to all intelligence information, services, and tools across multiple agencies and databases

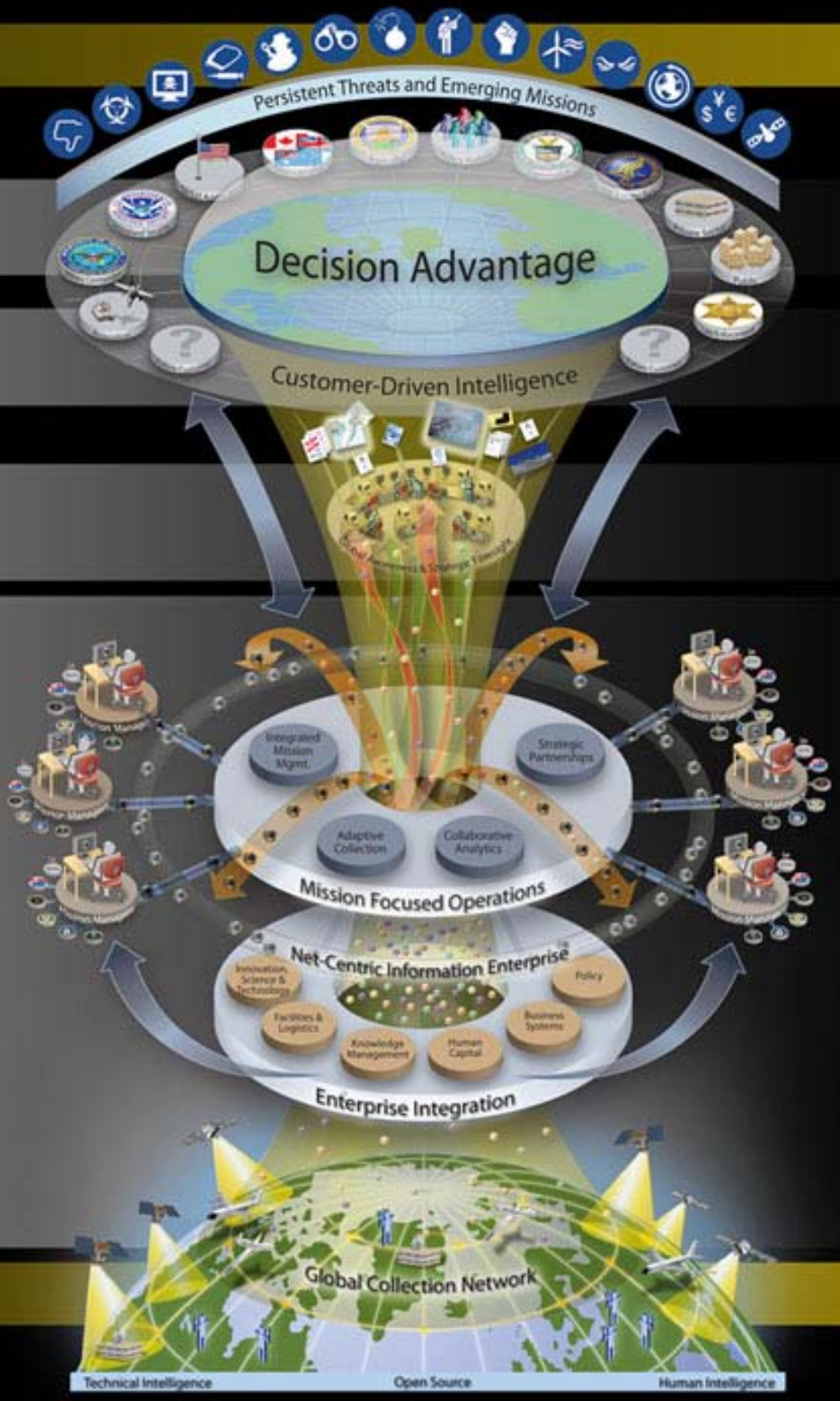
- Develop a common "cloud" based on a single backbone network and clusters of servers in scalable, distributed centers where data is stored, processed and managed
- Discover, access, and exploit data quickly and completely
- User-defined analytic environment through "drag and drop" composite applications
- Protects information from those who should not have it

Enterprise Integration

Creation of a strong institutional foundation that integrates the vital components of the Intelligence Enterprise – policy, people, processes, infrastructure, and technology – to remove the barriers to collaboration and reduce the "tooth-to-tail" ratio through greater economies of scale

A Globally Networked and Integrated Intelligence Enterprise

Director of National Intelligence
Washington DC, 20511


Persistent Threats and Emerging Missions
Decision Advantage
Customer-Driven Intelligence
Integrated Mission Mgmt.
Strategic Partnerships
Adaptive Collection
Collaborative Analytics
Mission Focused Operations
Net-Centric Information Enterprise
Innovation, Science & Technology
Policy
Facilities & Logistics
Business Systems
Knowledge Management
Human Capital
Enterprise Integration
Global Collection Network
Technical Intelligence
Open Source
Human Intelligence